

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

Download now

Read Online 

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

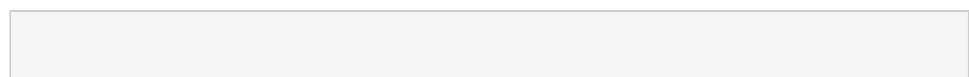
Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster.

The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data.

If you've never performed NSM analysis, *Applied Network Security Monitoring* will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job.

- Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus
- Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM



 [Download Applied Network Security Monitoring: Collection, D...pdf](#)

 [Read Online Applied Network Security Monitoring: Collection, ...pdf](#)

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster.

The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data.

If you've never performed NSM analysis, *Applied Network Security Monitoring* will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job.

- Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus
- Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith **Bibliography**

- Sales Rank: #131499 in eBooks
- Published on: 2013-11-26
- Released on: 2013-11-26
- Format: Kindle eBook

 [Download Applied Network Security Monitoring: Collection, D ...pdf](#)

 [Read Online Applied Network Security Monitoring: Collection, ...pdf](#)

Download and Read Free Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith

Editorial Review

Review

"... an extremely informative dive into the realm of network security data collection and analysis...well organized and thought through...I have only positive comments from my study." -*The Ethical Hacker Network*, Oct 31, 2014

About the Author

Chris Sanders is an information security consultant, author, and researcher originally from Mayfield, Kentucky. That's thirty miles southwest of a little town called Possum Trot, forty miles southeast of a hole in the wall named Monkey's Eyebrow, and just north of a bend in the road that really is named Podunk.

Chris is a Senior Security Analyst with InGuardians. He has an extensive experience supporting multiple government and military agencies, as well as several Fortune 500 companies. In multiple roles with the US Department of Defense, Chris significantly helped to further the role of the Computer Network Defense Service Provider (CNDSP) model, and helped to create several NSM and intelligence tools currently being used to defend the interests of the nation.

Chris has authored several books and articles, including the international best seller "Practical Packet Analysis" from No Starch Press, currently in its second edition. Chris currently holds several industry certifications, including the SANS GSE and CISSP distinctions.

In 2008, Chris founded the Rural Technology Fund. The RTF is a 501(c)(3) non-profit organization designed to provide scholarship opportunities to students from rural areas pursuing careers in computer technology. The organization also promotes technology advocacy in rural areas through various support programs. The RTF has provided thousands of dollars in scholarships and support to rural students.

When Chris isn't buried knee-deep in packets, he enjoys watching University of Kentucky Wildcat basketball, being a BBQ Pitmaster, amateur drone building, and spending time at the beach. Chris currently resides in Charleston, South Carolina with his wife Ellen.

Chris blogs at appliednsm.com and chrissanders.org. He is on Twitter as @chrissanders88.

Users Review

From reader reviews:

Melissa Sanders:

Reading a e-book tends to be new life style in this era globalization. With reading through you can get a lot of information that could give you benefit in your life. Along with book everyone in this world can certainly share their idea. Books can also inspire a lot of people. Many author can inspire their very own reader with their story as well as their experience. Not only situation that share in the guides. But also they write about the information about something that you need example. How to get the good score toefl, or how to teach your kids, there are many kinds of book which exist now. The authors on this planet always try to improve

their skill in writing, they also doing some analysis before they write on their book. One of them is this Applied Network Security Monitoring: Collection, Detection, and Analysis.

Bruce Benedict:

Applied Network Security Monitoring: Collection, Detection, and Analysis can be one of your basic books that are good idea. Many of us recommend that straight away because this e-book has good vocabulary that will increase your knowledge in terminology, easy to understand, bit entertaining but nevertheless delivering the information. The article writer giving his/her effort to set every word into joy arrangement in writing Applied Network Security Monitoring: Collection, Detection, and Analysis yet doesn't forget the main level, giving the reader the hottest along with based confirm resource facts that maybe you can be among it. This great information can easily drawn you into completely new stage of crucial pondering.

Fredrick Alfred:

Your reading 6th sense will not betray an individual, why because this Applied Network Security Monitoring: Collection, Detection, and Analysis guide written by well-known writer who really knows well how to make book that may be understand by anyone who read the book. Written throughout good manner for you, dripping every ideas and publishing skill only for eliminate your current hunger then you still hesitation Applied Network Security Monitoring: Collection, Detection, and Analysis as good book not merely by the cover but also from the content. This is one e-book that can break don't ascertain book by its deal with, so do you still needing one more sixth sense to pick that!? Oh come on your looking at sixth sense already told you so why you have to listening to yet another sixth sense.

Kristy Abrahams:

This Applied Network Security Monitoring: Collection, Detection, and Analysis is completely new way for you who has fascination to look for some information because it relief your hunger of knowledge. Getting deeper you onto it getting knowledge more you know otherwise you who still having tiny amount of digest in reading this Applied Network Security Monitoring: Collection, Detection, and Analysis can be the light food for you because the information inside this book is easy to get through anyone. These books produce itself in the form which is reachable by anyone, yes I mean in the e-book form. People who think that in e-book form make them feel drowsy even dizzy this guide is the answer. So there isn't any in reading a e-book especially this one. You can find actually looking for. It should be here for you actually. So , don't miss the item! Just read this e-book kind for your better life and knowledge.

Download and Read Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith #JRZ8EDPVK10

Read Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith for online ebook

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith books to read online.

Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith ebook PDF download

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Doc

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Mobipocket

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith EPub

JRZ8EDPVK10: Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith